SHIV SHAKTI

International Journal in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 7, No. 2, April 2018 (ISSN 2278 – 5973)

Security And Privacy Enhancing Multicloud Architecture

A.RACHANA

Department of Computer Science
HITAM, Jntuh
Hyderabad, India.

P.PRIYANKA

Department of Computer Science
HITAM, Jntuh
Hyderabad, India.

K.AKHILA

Department of Computer Science
HITAM, Jntuh
Hyderabad, India.

D. VAMSHIDHAR

Department of Computer Science
HITAM, Jntuh
Hyderabad, India.

NAVAKISHORE

Assistant Professor

Department of CSE

HITAM, Jntuh

Hyderabad, India.

Abstract— In last few years use of Cloud Computing in different modes like cloud storage, cloud hosting, cloud servers are increased in industries and other organizations as per requirements. The Security challenges are still among the biggest obstacles when considering the adoption of cloud services. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Key exposure is one serious security problem for cloud storage auditing. Alongside with these security issues, the cloud paradigm comes with a new set of unique and different features, which open the path toward novel security approaches, techniques, and architectures. This work provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

Index Terms—Key exposure, data confidentiality, dispersed storage.

1. INTRODUCTION

The world recently witnessed a massive surveillance program aimed at breaking users privacy. Perpetrators were not hindered by the various security measures deployed within the targeted services .In order to deal with this problem, cloud storage auditing scheme with exposure resilience has been proposed. For instance, although these services relied on encryption mechanisms to guarantee data confidentiality, the necessary keying material was acquired by means of backdoors, bribe, or coercion.

If the encryption key is exposed, the only viable means to guarantee confidentiality is to limit the adversary's access to the cipher text, e.g., by spreading it across multiple administrative domains, in the hope that the adversary cannot compromise all of them. However, even if the data is encrypted and dispersed across different administrative domains, an adversary equipped with the appropriate keying material can compromise a server in one domain and decrypt cipher-text blocks stored therein.

In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the cipher text blocks. The adversary can acquire the key either by exploiting flaws or backdoors or mistakes in the key-generation software, or by compromising the devices that store the keys (e.g., at the user-side or in the cloud). As far as we are aware of that, this adversary invalidates the security of most cryptographic solutions, including those that protect encryption keys by means of secret)-sharing (since these keys can be leaked as soon as they are generated).

2. EXISTING SYSTEM

- $(n - \lambda)$**key exposure security** notions for encryption modes capture data confidentiality against an adversary which does not have the encryption key. That is, if the key is leaked, the confidentiality of data is broken.

- In the *ind* experiment, the adversary has unrestricted access to data during the "find" stage. At this point, A outputs two messages of equal length x0, x1,and some state information that are

passed as input when the adversary is initialized for the "guess" stage(e.g., state can contain the two messages x0, x1). During the "guess" stage, the adversary is given the cipher text of one message out of x0, x1 and must guess which message was actually encrypted.

3. PROBLEM DEFINITION

We propose Bastion, an efficient scheme which ensures data confidentiality against an adversary that knows the encryption key and has access to a large fraction of the cipher text blocks. We analyze the security of Bastion, and we show that it prevents leakage of any plaintext block as long as the adversary has access to the encryption key and to all but two cipher text blocks.

4. PROPOSED SYSTEM

- In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the cipher text blocks.
- The adversary can acquire the key either by exploiting flaws or backdoors in the key-generation software, or by compromising the devices that store the keys (eg . ,at the user-side or in the cloud).
- As far as we are aware, this adversary invalidates the security of most cryptographic solutions, including those that protect encryption keys by means of secret-sharing (since these keys can be leaked as soon as they are generated).
- To counter such an adversary, we propose Bastion, a novel and efficient scheme which ensures that plaintext data cannot be recovered as long as the adversary has access to at most all but *two* cipher text blocks, even when the encryption key is exposed.
- In this paper,we innovatively propose a paradigm name strong key exposure resilient auditing for secure cloud storage.
- In our proposed scheme, the key exposure in one time period does not affect the security of cloud storage in other time periods.

5. MODULES

5.1. Owner Module Has Following Functionalities:

- Data Upload
- Upload Files Into Two Clouds.
- View Uploaded Files

5.2. User Module Has Following Functionalities:

- View Files And Send Request
- Verify The Keys Sent
- Download The Files

5.3. Cloud-A Module Has Following Functionalities:

- View Files Uploaded By User
- Provide Private Key
- View The Part 0 File

5.4. Cloud-B Module Has Following Functionalities:

- View User Requests
- Send Keys to User
- View The Part 1 File

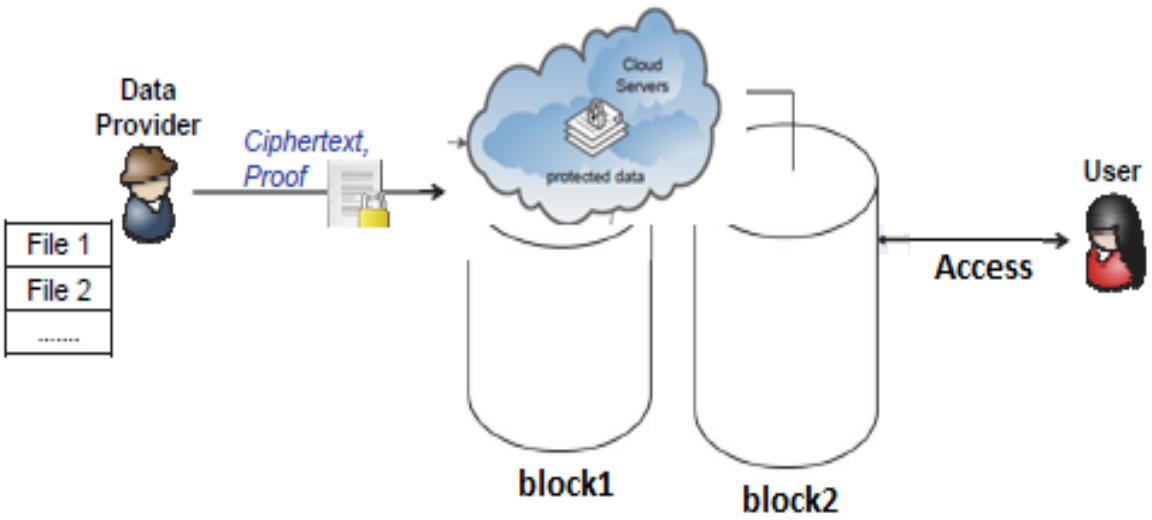

Fig.no.1. System Architecture.

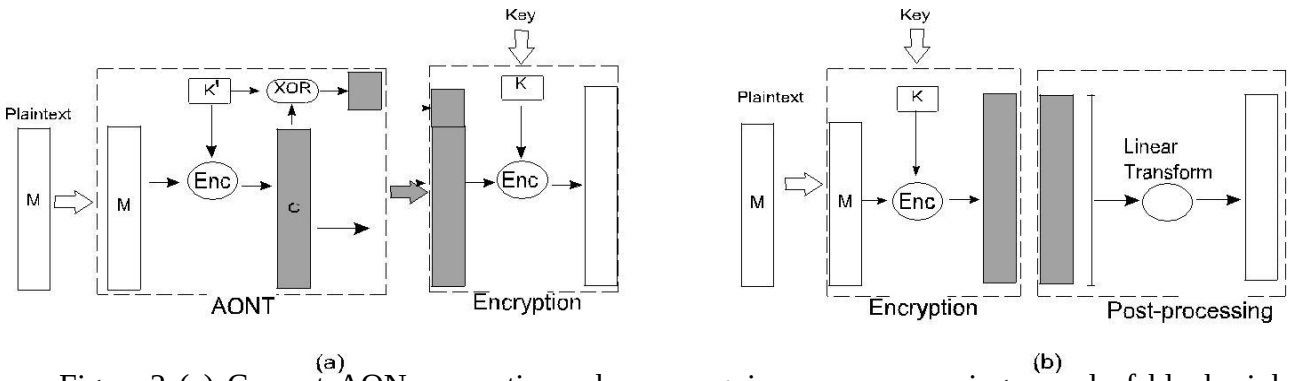

Fig.no.2 (a) Current AON encryption schemes require a pre-processing round of block cipher encryption for the AONT, followed by another round of block cipher encryption.
Fig.no.2 (b) On the other hand, BASTION first encrypts the data with one round of block cipher encryption, and then applies an efficient linear post-processing to the cipher text.

6. CONCLUSION

We addressed the problem of securing data outsourced to the cloud against an adversary which has access to the encryption key. For that purpose, we introduced a novel security definition that captures data confidentiality against the new adversary. We then proposed Bastion, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but *two* cipher text blocks.

7. ACKNOWLEDGMENT

It gives us great pleasure in presenting the final project report on "SECURITY AND PRIVACY ENHANCING MULTICLOUD ARCHITECTURE". We would like to take this opportunity to thank our internal guide **Prof.Dr. Pushpender Sarao** and **H.O.D Dr. Ila Chandana Kumari** for giving us all the help and guidance we needed.We are really grateful to them for their kind support.Their valuable suggestions were very helpful.

8. REFERENCES

[1] S. Micali and L. Reyzin, "Physically observable cryptography (extended abstract)," in *Theory of Cryptography Conference (TCC)*, 2004, pp. 278–296.

[2] NEC Corp., "HYDRAstor Grid Storage," http://www. hydrastor.com.

[3] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, 1989.

[4] J. K. Resch and J. S. Plank, "AONT- RS: Blending Security and Performance in Dispersed Storage Systems," in *USENIX Conference on File and Storage Technologies (FAST)*, 2011, pp. 191–202.